Advanced Topics: Scaling, Exploits, and Security

Mini-Lecture (30 minutes)

Prof. Dr. Jörg Osterrieder · Blockchain, Crypto Economy & NFTs · Spring 2026

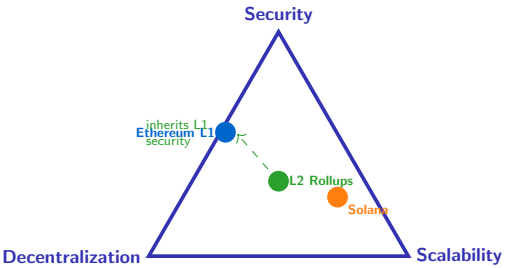
Learning Objectives:

1. **[Understand]** Explain how L2 rollups solve the scalability trilemma
2. **[Analyze]** Compare optimistic and ZK-rollups on security and finality
3. **[Apply]** Trace a flash loan attack and identify the exploit vector
4. **[Evaluate]** Apply the 5-Layer Security Framework to evaluate protocol risk

Topics: Layer-2 Scaling · Flash Loans · Smart Contract Security · MEV · Bridge Attacks

By the end of this session you will be able to reason about protocol design trade-offs and evaluate DeFi security postures.

The Scalability Trilemma and L2 Solutions



Three L2 Approaches:

Type	How it Works
Rollups	Off-chain execution; data + proof posted to L1. Optimistic or ZK.
Sidechains	Independent chain with own validators (e.g., Polygon).
State Channels	Bilateral off-chain; settle on-chain at close (e.g., Lightning).

Key Insight

Rollups inherit Ethereum's security while achieving 10–100× throughput gains.

Trilemma: no single layer optimizes all three — L2 solutions trade off one property to gain another.

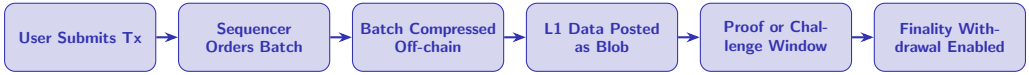
Optimistic vs. ZK-Rollups: Head-to-Head

Dimension	Optimistic Rollup	ZK-Rollup
How it works	Assume batch valid; fraud proof submitted by watchers if invalid	Validity proof (ZK-SNARK/STARK) generated off-chain, verified on L1
Finality	∼**7 days** (challenge window must elapse)	**Minutes** (proof verified on L1 immediately)
Security model	1-of-N honest verifier assumed to submit fraud proof	Cryptographic soundness; trustless (no honesty assumption)
Examples	Arbitrum, Optimism, Base	Starknet, zkSync Era, Scroll
Key trade-off	EVM-compatible, easy migration; but slow L1 withdrawals	Fast finality; but high proving cost and EVM complexity

Post-Dencun (EIP-4844, March 2024): Both rollup types now post data as *blob transactions* rather than calldata, reducing L1 data costs by up to 98%. Base fees dropped from $0.50 to $0.005 per transaction overnight.

Optimistic rollups dominate TVL today (Arbitrum, Base); ZK-rollups are growing as proving costs fall with hardware acceleration.

How a Rollup Works: Transaction Lifecycle



Optimistic: Fraud proof window = 7 days before withdrawal to L1

ZK: Validity proof generated in minutes, then immediately final on L1

Centralisation Risk

Most rollups today use a **single sequencer** – a bottleneck and censorship risk. Decentralised sequencer sets are an active research area.

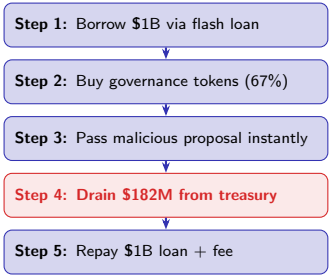
Dencun Impact (March 2024)

Blob transactions (EIP-4844) cut rollup L1 data costs by up to 98%. Base daily fees dropped from **$**1M+ to under **$**20K.

The sequencer is the current centralisation risk in most rollups – decentralised sequencers are an active research area (Espresso, Astria).

Flash Loans: Zero-Capital Attacks

Beanstalk Attack (April 2022)



All in one transaction ($\approx$13 seconds)

What Makes Flash Loans Dangerous?

- **Zero capital required:** Any amount, no collateral
- **Atomic:** Borrow, exploit, repay in one tx
- **Reversible on failure:** If repayment fails, entire tx reverts – attacker loses only gas
- **Speed:** Governance, oracle manipulation in $<$30 seconds

Flash Loan Attack Patterns:

1. **Oracle manipulation:** Inflate price on DEX, exploit lending protocol
2. **Governance attacks:** Instant majority for malicious vote (Beanstalk)
3. **Arbitrage:** Legitimate – capture price diffs across pools
4. **Collateral swaps:** Replace collateral in a single block

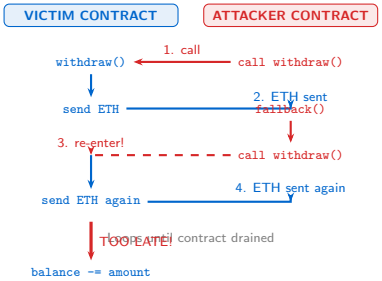
Defence

Time-weighted average prices (TWAPs), timelocks on governance, multi-block oracle readings.

Flash loans are not inherently malicious – they enable arbitrage, collateral swaps, and self-liquidation. The attack vector is the exploited protocol's logic.

Smart Contract Vulnerabilities: Reentrancy

The Call Sequence (Recursive Drain)



The Bug: Wrong Execution Order

- **Vulnerable pattern:** Send ETH *before* updating balance
- **Attacker's trick:** `fallback()` re-calls `withdraw()` before balance is updated
- **Result:** Contract drained completely

The DAO Hack (2016)

3.6M ETH stolen (≈$60M at the time) using exactly this pattern. Led to Ethereum hard fork creating ETH and ETC.

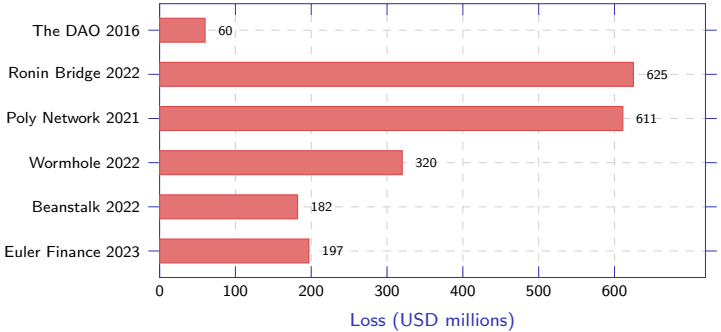
Fix: Checks-Effects-Interactions Pattern

1. **Check:** `require(balance[msg.sender] > 0)`
2. **Effect:** `balance[msg.sender] = 0` *(first!)*
3. **Interact:** `msg.sender.call{value: amount}("")`

Also: use `ReentrancyGuard` (OpenZeppelin) or `nonReentrant` modifier.

Reentrancy remains in the OWASP Smart Contract Top 10 nearly a decade after The DAO. The fix is simple – the pattern is easy to overlook under deadline pressure.

Major Smart Contract Exploits: The Billion-Dollar Bug Timeline



Attack Vectors:

DAO	Reentrancy
Poly	Access control
Ronin	Key theft (5/9)
Wormhole	Signature bug
Beanstalk	Flash loan
Euler	Flash loan + bug

Total

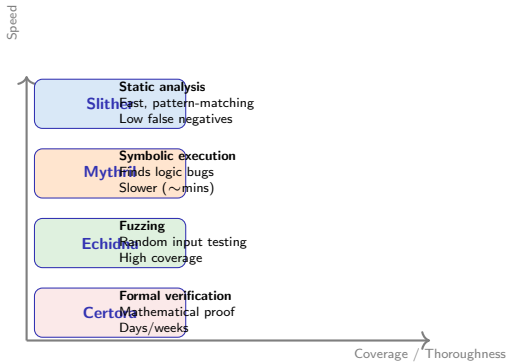
shown: $1.995B

DeFi hacks 2016–2024: >**$3 billion**

No single attack type dominates – bridge attacks, access control failures, and flash loan exploits each account for major losses.

Security Tools and the Audit Process

Four Complementary Security Tools:



5-Step Audit Pipeline:

1. **Automated Scan** (Slither, Mythril)
   Catch known patterns in minutes
2. **Fuzz Testing** (Echidna)
   Explore edge cases with random inputs
3. **Manual Code Review**
   Senior auditors: logic & business risk
4. **Formal Verification** (Certora)
   Prove invariants mathematically
5. **Bug Bounty** (Immunefi, HackerOne)
   Crowdsource ongoing discovery

Warning

A single audit is insufficient. The Euler Finance hack ($197M) occurred despite a prior audit. Continuous monitoring is essential.

Security is a process, not a one-time event. The cost of a thorough audit ($50–500K) is trivial compared to the cost of a hack.

MEV, Bridges, and Cross-Chain Risk

Maximal Extractable Value (MEV)

MEV is profit extracted by block producers (or searchers) by reordering, inserting, or censoring transactions.

- **Sandwich attack:** Searcher sees large pending swap; inserts buy *before* it and sell *after* – user gets a worse price
- **Front-running:** Copy a profitable arbitrage tx with higher gas
- **Back-running:** Place tx immediately after a known large trade
- **Scale:** >$600M extracted on Ethereum (2020–2025, cumulative)

Why Bridges Are the Weakest Link

Bridges lock assets on one chain and mint equivalents on another – a concentrated honeypot.

Bridge	Loss	Attack
Ronin	$625M	Validator key theft (5 of 9)
Wormhole	$320M	Signature verification bug
Nomad	$190M	Merkle root initialisation
Harmony	$100M	2-of-5 multisig compromised

Mitigations

MEV-Boost (PBS), commit-reveal schemes, private mempools (Flashbots Protect), slippage limits.

Root Cause Pattern

Bridges concentrate trust in few validators or rely on bespoke cryptography – the antithesis of the security-by-decentralisation model of L1s.

MEV and bridge attacks represent systemic risks that grow with DeFi TVL – they scale with the value they can extract.

Key Takeaways

1. **L2 rollups solve the scalability trilemma by inheriting L1 security.**
   The Dencun upgrade (March 2024, EIP-4844 blob transactions) cut rollup fees by up to 98%. Optimistic rollups have 7-day withdrawal delays; ZK-rollups settle in minutes with cryptographic proofs.

2. **Flash loans enable zero-capital attacks – atomic, reversible, and devastatingly fast.**
   The Beanstalk exploit ($182M) borrowed $1B, seized governance, and drained the treasury in a single 13-second transaction. Defence requires TWAPs, governance timelocks, and multi-block oracles.

3. **Over $3 billion lost to smart contract exploits – reentrancy, oracle manipulation, bridge attacks.**
   The DAO (2016) established reentrancy as a foundational vulnerability. Bridges are the single largest attack surface, concentrating trust that L1s deliberately distribute.

4. **Defence requires multiple layers: automated scanning + manual audit + bug bounties + formal verification.**
   No single tool catches all bugs. A rigorous 5-step pipeline (Scan $\rightarrow$ Fuzz $\rightarrow$ Review $\rightarrow$ Verify $\rightarrow$ Bounty) combined with on-chain monitoring is the industry standard.

Cryptoeconomic design must account for adversarial conditions: assume attackers are rational, well-capitalised, and faster than you.

Quiz: Advanced Topics (Q1–Q5)

Q1. [Understand] What three properties does the scalability trilemma force a trade-off between?
A) Speed, Cost, Privacy B) Security, Scalability, Decentralization C) Throughput, Latency, Finality D) Consensus, Sharding, Rollups

Quiz: Advanced Topics (Q1–Q5)

Q1. [Understand] What three properties does the scalability trilemma force a trade-off between?
A) Speed, Cost, Privacy B) Security, Scalability, Decentralization C) Throughput, Latency, Finality D) Consensus, Sharding, Rollups
Answer: B – The trilemma states that a blockchain can optimise at most two of: Security, Scalability, Decentralization.

Q2. [Apply] An optimistic rollup batch is submitted to L1. How long must users wait before withdrawing to L1?
A) 1 hour B) 24 hours C) 7 days D) 30 days

Quiz: Advanced Topics (Q1–Q5)

Q1. [Understand] What three properties does the scalability trilemma force a trade-off between?
A) Speed, Cost, Privacy B) Security, Scalability, Decentralization C) Throughput, Latency, Finality D) Consensus, Sharding, Rollups
Answer: B – The trilemma states that a blockchain can optimise at most two of: Security, Scalability, Decentralization.

Q2. [Apply] An optimistic rollup batch is submitted to L1. How long must users wait before withdrawing to L1?
A) 1 hour B) 24 hours C) 7 days D) 30 days
Answer: C – The 7-day challenge window allows fraud proofs to be submitted before withdrawal is finalised.

Q3. [Apply] A flash loan attack borrows $500M, manipulates an oracle, drains $50M, then the repayment step fails. What happens?
A) Attacker keeps the $50M B) Attacker loses only the gas fee C) Entire transaction reverts D) Protocol is paused automatically

Quiz: Advanced Topics (Q1–Q5)

Q1. [Understand] What three properties does the scalability trilemma force a trade-off between?
A) Speed, Cost, Privacy B) Security, Scalability, Decentralization C) Throughput, Latency, Finality D) Consensus, Sharding, Rollups
Answer: B – The trilemma states that a blockchain can optimise at most two of: Security, Scalability, Decentralization.

Q2. [Apply] An optimistic rollup batch is submitted to L1. How long must users wait before withdrawing to L1?
A) 1 hour B) 24 hours C) 7 days D) 30 days
Answer: C – The 7-day challenge window allows fraud proofs to be submitted before withdrawal is finalised.

Q3. [Apply] A flash loan attack borrows $500M, manipulates an oracle, drains $50M, then the repayment step fails. What happens?
A) Attacker keeps the $50M B) Attacker loses only the gas fee C) Entire transaction reverts D) Protocol is paused automatically
Answer: C – Flash loans are atomic: if repayment fails, the entire transaction (including the drain) reverts – attacker only loses gas.

Q4. [Analyze] Why are bridges particularly vulnerable compared to L1 smart contracts?
A) They use older Solidity versions B) Concentrated trust in few validators C) They don't use cryptography D) Bridges can't be audited

Quiz: Advanced Topics (Q1–Q5)

Q1. [Understand] What three properties does the scalability trilemma force a trade-off between?
A) Speed, Cost, Privacy B) Security, Scalability, Decentralization C) Throughput, Latency, Finality D) Consensus, Sharding, Rollups
Answer: B – The trilemma states that a blockchain can optimise at most two of: Security, Scalability, Decentralization.

Q2. [Apply] An optimistic rollup batch is submitted to L1. How long must users wait before withdrawing to L1?
A) 1 hour B) 24 hours C) 7 days D) 30 days
Answer: C – The 7-day challenge window allows fraud proofs to be submitted before withdrawal is finalised.

Q3. [Apply] A flash loan attack borrows $500M, manipulates an oracle, drains $50M, then the repayment step fails. What happens?
A) Attacker keeps the $50M B) Attacker loses only the gas fee C) Entire transaction reverts D) Protocol is paused automatically
Answer: C – Flash loans are atomic: if repayment fails, the entire transaction (including the drain) reverts – attacker only loses gas.

Q4. [Analyze] Why are bridges particularly vulnerable compared to L1 smart contracts?
A) They use older Solidity versions B) Concentrated trust in few validators C) They don't use cryptography D) Bridges can't be audited
Answer: B – Bridges create concentrated trust points (e.g., 5-of-9 validators in Ronin) that are high-value targets.

Q5. [Apply] In a reentrancy attack, what is the critical programming mistake?
A) Using too much gas B) Failing to emit events C) State (balance) updated after the external call D) Missing access control

Quiz: Advanced Topics (Q1–Q5)

Q1. [Understand] What three properties does the scalability trilemma force a trade-off between?
A) Speed, Cost, Privacy B) Security, Scalability, Decentralization C) Throughput, Latency, Finality D) Consensus, Sharding, Rollups
Answer: B – The trilemma states that a blockchain can optimise at most two of: Security, Scalability, Decentralization.

Q2. [Apply] An optimistic rollup batch is submitted to L1. How long must users wait before withdrawing to L1?
A) 1 hour B) 24 hours C) 7 days D) 30 days
Answer: C – The 7-day challenge window allows fraud proofs to be submitted before withdrawal is finalised.

Q3. [Apply] A flash loan attack borrows $500M, manipulates an oracle, drains $50M, then the repayment step fails. What happens?
A) Attacker keeps the $50M B) Attacker loses only the gas fee C) Entire transaction reverts D) Protocol is paused automatically
Answer: C – Flash loans are atomic: if repayment fails, the entire transaction (including the drain) reverts – attacker only loses gas.

Q4. [Analyze] Why are bridges particularly vulnerable compared to L1 smart contracts?
A) They use older Solidity versions B) Concentrated trust in few validators C) They don't use cryptography D) Bridges can't be audited
Answer: B – Bridges create concentrated trust points (e.g., 5-of-9 validators in Ronin) that are high-value targets.

Q5. [Apply] In a reentrancy attack, what is the critical programming mistake?
A) Using too much gas B) Failing to emit events C) State (balance) updated after the external call D) Missing access control
Answer: C – The fix is Checks-Effects-Interactions: update state *before* making any external calls.

Answers hidden initially – reveal with presenter click. All questions map directly to the four learning objectives.

Quiz: Advanced Topics (Q6–Q10)

Q6. [Understand] What did the Dencun upgrade (March 2024) introduce to reduce L2 fees?
A) State channels B) Blob transactions (proto-danksharding, EIP-4844) C) Recursive ZK proofs D) Validator sharding

Quiz: Advanced Topics (Q6–Q10)

Q6. [Understand] What did the Dencun upgrade (March 2024) introduce to reduce L2 fees?
A) State channels B) Blob transactions (proto-danksharding, EIP-4844) C) Recursive ZK proofs D) Validator sharding
Answer: B – EIP-4844 added blob-carrying transactions, reducing L1 data costs for rollups by up to 98%.

Q7. [Analyze] A sandwich attack profits by trading before AND after a user's large swap. Who bears the cost?
A) The block validator B) The liquidity provider C) The user receives a worse execution price D) The protocol treasury

Quiz: Advanced Topics (Q6–Q10)

Q6. [Understand] What did the Dencun upgrade (March 2024) introduce to reduce L2 fees?
A) State channels B) Blob transactions (proto-danksharding, EIP-4844) C) Recursive ZK proofs D) Validator sharding
Answer: B – EIP-4844 added blob-carrying transactions, reducing L1 data costs for rollups by up to 98%.

Q7. [Analyze] A sandwich attack profits by trading before AND after a user's large swap. Who bears the cost?
A) The block validator B) The liquidity provider C) The user receives a worse execution price D) The protocol treasury
Answer: C – The user's effective price worsens because the attacker's front-run pushes the price up before the user's swap executes.

Q8. [Apply] Which security tool is the fastest but provides the lowest coverage?
A) Certora B) Echidna C) Mythril D) Slither

Quiz: Advanced Topics (Q6–Q10)

Q6. [Understand] What did the Dencun upgrade (March 2024) introduce to reduce L2 fees?
A) State channels B) Blob transactions (proto-danksharding, EIP-4844) C) Recursive ZK proofs D) Validator sharding
Answer: B – EIP-4844 added blob-carrying transactions, reducing L1 data costs for rollups by up to 98%.

Q7. [Analyze] A sandwich attack profits by trading before AND after a user's large swap. Who bears the cost?
A) The block validator B) The liquidity provider C) The user receives a worse execution price D) The protocol treasury
Answer: C – The user's effective price worsens because the attacker's front-run pushes the price up before the user's swap executes.

Q8. [Apply] Which security tool is the fastest but provides the lowest coverage?
A) Certora B) Echidna C) Mythril D) Slither
Answer: D – Slither is a fast static analyser that catches known patterns in seconds but misses complex logic bugs.

Q9. [Evaluate] A protocol has $200M TVL, one prior audit six months ago, and no bug bounty. Rate its security posture.
A) Strong – one audit is sufficient B) Adequate – TVL proves trust C) Weak – single audit and no bounty is insufficient D) Cannot assess without source code

Quiz: Advanced Topics (Q6–Q10)

Q6. [Understand] What did the Dencun upgrade (March 2024) introduce to reduce L2 fees?
A) State channels B) Blob transactions (proto-danksharding, EIP-4844) C) Recursive ZK proofs D) Validator sharding
Answer: B – EIP-4844 added blob-carrying transactions, reducing L1 data costs for rollups by up to 98%.

Q7. [Analyze] A sandwich attack profits by trading before AND after a user's large swap. Who bears the cost?
A) The block validator B) The liquidity provider C) The user receives a worse execution price D) The protocol treasury
Answer: C – The user's effective price worsens because the attacker's front-run pushes the price up before the user's swap executes.

Q8. [Apply] Which security tool is the fastest but provides the lowest coverage?
A) Certora B) Echidna C) Mythril D) Slither
Answer: D – Slither is a fast static analyser that catches known patterns in seconds but misses complex logic bugs.

Q9. [Evaluate] A protocol has $200M TVL, one prior audit six months ago, and no bug bounty. Rate its security posture.
A) Strong – one audit is sufficient B) Adequate – TVL proves trust C) Weak – single audit and no bounty is insufficient D) Cannot assess without source code
Answer: C – A single audit is point-in-time. Euler Finance ($197M hack) had been audited. Continuous bug bounties and monitoring are essential.

Q10. [Analyze] Why can't the classic DAO reentrancy pattern work against a contract using Checks-Effects-Interactions?
A) CEI contracts reject external calls B) The balance is set to zero before ETH is sent, so re-entry finds no funds C) CEI uses a mutex lock D) Fallback functions are disabled

Quiz: Advanced Topics (Q6–Q10)

Q6. [Understand] What did the Dencun upgrade (March 2024) introduce to reduce L2 fees?
A) State channels B) Blob transactions (proto-dankssharding, EIP-4844) C) Recursive ZK proofs D) Validator sharding
Answer: B – EIP-4844 added blob-carrying transactions, reducing L1 data costs for rollups by up to 98%.

Q7. [Analyze] A sandwich attack profits by trading before AND after a user's large swap. Who bears the cost?
A) The block validator B) The liquidity provider C) The user receives a worse execution price D) The protocol treasury
Answer: C – The user's effective price worsens because the attacker's front-run pushes the price up before the user's swap executes.

Q8. [Apply] Which security tool is the fastest but provides the lowest coverage?
A) Certora B) Echidna C) Mythril D) Slither
Answer: D – Slither is a fast static analyser that catches known patterns in seconds but misses complex logic bugs.

Q9. [Evaluate] A protocol has $200M TVL, one prior audit six months ago, and no bug bounty. Rate its security posture.
A) Strong – one audit is sufficient B) Adequate – TVL proves trust C) Weak – single audit and no bounty is insufficient D) Cannot assess without source code
Answer: C – A single audit is point-in-time. Euler Finance ($197M hack) had been audited. Continuous bug bounties and monitoring are essential.

Q10. [Analyze] Why can't the classic DAO reentrancy pattern work against a contract using Checks-Effects-Interactions?
A) CEI contracts reject external calls B) The balance is set to zero before ETH is sent, so re-entry finds no funds C) CEI uses a mutex lock D) Fallback functions are disabled
Answer: B – CEI updates state (balance = 0) before the external call, so any re-entrant `withdraw()` sees zero balance and reverts.

Score 8–10: Expert level. 5–7: Solid foundation. Below 5: Review reentrancy, rollup mechanics, and flash loan atomicity.